Remarks

1. Claims 1-21 are pending.

2. Claims 1, 3, 6, 7, 8, 12, 18 and 20 stand objected to for the following informalities:

"Claim 1 recites the limitation "the secret" in line 16. Claim 3 recites the limitation "the symmetric" in line 3. Claim 6 recites the limitation "the hash" in line 3 and "the first" in line 5. Claim 8 recites the limitation "the value" in line 6, and "the authenticator" in line 19. Claim 12 recites the limitation "the hash" in line 3. Claim 18 recites the limitation "the identifier" in line 4, "the public" in line 5, "the password" in line 9, "the token" in line 10, and "the successful" in line 14. Claim 20 recites the limitation "the encrypted value" in line 10. There are insufficient antecedent basis for these limitations in the claims."

3. Claims 1-7, 18 and 19 stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

"Claim 1 includes: "(d) the subscriber station receiving an authenticator of the authentication server according to an authentication success on the transmitted authenticator of the subscriber by the authentication server; and (e) the subscriber station using the secret key and the password, authenticating the received authenticator of the authentication server, and receiving the authenticator of the authentication server when the authentication is successful". The meaning and scope of these limitations are unclear. For example it is not clear in step (d) "according to an authentication success" is referring to what/which "authentication success". Claim does not show any step for authentication success. Step (d) discloses "receiving an authenticator of the authentication server ". Step (e) also discloses "receiving the authenticator of the authentication server". It is not clear as why authenticator of the authentication server is received in both steps (d) and (e).

Claim 18 stands rejected under 35 U.S.C. 112, second paragraph for including unclear limitations similar to the claim 1. Claims 2-7 and 19 stands rejected under 35 U.S.C. 112, second paragraph, for being dependent on the rejected claims 1 and 18. "

4. Claims 1-21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Halasz et al. (US Patent No. 6,996,714) in view of Mackenzie (US Publication No. 2002/0194478).

5. Claims 1, 3, 6, 8, 12, 15, 18 and 20 have been amended. No new matter has been added.

6. Formality Objections and Rejections under 35 U.S.C. 112

Claims 1, 3, 6, 7, 8, 12, 18 and 20 stand objected to for informalities.

Claims 1-7, 18 and 19 stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 3, 6, 8, 12, 15, 18 and 20 have been amended.

Applicants submit that the amendments to the claims make the Examiner's objections and the rejection under 35 U.S.C. 112 now moot.

7. Rejections under 35 U.S.C. 103(a)

Claims 1-21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Halasz et al. (US Patent No. 6,996,714) in view of Mackenzie (US Publication No. 2002/0194478).

Applicants have reviewed the Halasz and Mackensie references with care, paying particular attention to the passages cited, and submit that claims 1, 8, 15, 18 and 20 as amended are not obvious in view of these references.

Halasz teaches in col. 7 line 35 to col. 8 line 7 quoted below that a server transmits "vendor-specific attributed indicating a key value" to a client for authenticating the server by the

client and the client authenticates the server using the "vendor-specific attributed indicating a key value".

"Referring now to FIG. 3, there is illustrated a general flow chart of the protocol process for mutual authentication between the wireless client 106 and AS 110 of FIG. 1a. Flow begins at a Start terminal and moves to a function block 300 where the client 106 associates to the AP 102. The AP 102 then sends an EAP identity request to the client 106, as indicated in a function block 302. Flow is to a function block 304 where the username and password of the client user are obtained (e.g., via a login process) in the client 106. The username is transmitted from the client 106 to the AP 102, and forwarded from the AP 102 to the AS 110. The AS 110 then issues a challenge to the client 106, as indicated in a function block 306. In a function block 308, the client 106 responds by performing a DES encryption step, and sending the DES encrypted data to the AS 110. The AS 110 does the same DES encryption based on information corresponding to the received username and checks it against the encrypted response data received from the client 106. Flow is then to a decision block 312 where if the client 106 is not a valid client, flow is out the "N" path to a function block 314 to deny network access to the client 106. Flow then loops back to the input of function block 300 to reinitiate the association process. If the AS 110 determines that the client is valid, flow is out the "Y" path of decision block 312 where the AS 110 notifies the AP 102 that the client is valid, which AP 102 forwards the validation information to the client 106.

In accordance with the mutual authentication aspects of the disclosed LEAP algorithm, the client 106 then initiates a challenge to the AS 110, as indicated in a function block 318. Flow is to a function block 320 where the AS 110 responds with an access-accept, and *vendor-specific attribute indicating a key value. This response is forwarded to the client 106 who then performs validation of the network, as indicated in a function block 322.* Flow is to a decision block 324, where if the client 106 does not validate the network, flow is out the "N" path to a function block 326 where the client 106 disassociates with the network. Flow then loops back to the input of function block 300 where the client 106 can then be forced to reinitiate the association process."

Applicant submits therefore that Halasz teaches away from "*transmitting the encrypted first predetermined value and a generated authenticator of the subscriber to the authentication server; (d) the subscriber station receiving the authentication server's authenticator from the authentication server which authenticates the generated authenticator of the subscriber using the encrypted first predetermined value and generates the authentication server's authenticator when the authentication is successful; and (e) the subscriber station using a secret key and the password, authenticating the received authenticator of the authentication server, and accepting the authenticator of the authentication server when the authentication is successful, wherein the authentication server's authenticator is generated by the authentication server using the encrypted first predetermined value transmitted from the subscriber station, and wherein the*

subscriber station authenticates the authentication server's authenticator using the first predetermined value", as recited in claim 1 and similarly in claims 8, 15, 18, and 20.

Claims 1, 8, 15, 18, and 20 have the feature that a server generates the server's authenticator using an encrypted value transmitted from a client and transmits "the server's authenticator" to the client, and the client authenticates "the server's authenticator" transmitted from the server using a value that is encrypted by the client and becomes the encrypted value.

As described above, in Halasz, the server transmits "vendor-specific attributed indicating a key value", which is unrelated to the client and is unique to the server. Therefore Applicant submits that Halasz teaches away from the server transmitting the authentication server's authenticator generated by the client using the value related to the client, as claimed, because Halasz teaches transmitting a different "vendor-specific attributed indicating a key value" to the client.

Thus Applicants submit that claims 1, 8, 15, 18 and 20 as amended are not obvious in view of and are patentable over Halasz and Mackensie.

.

Should the Examiner disagree, Applicants respectfully request him to clearly and specifically point out where any of these references disclose or make obvious these features in accordance with 37 C.F.R. 1.104(c)2.

8. Dependent Claims

Claims 2-7, 9-14, 16-17, 19 and 21 depend on independent claims 1, 8, 15, 18 or 20. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion, Applicants submit that these dependent claims are also allowable at least by virtue of their dependency on nonobvious claims as well as the additional limitations recited by each of these claims.

Conclusion

In view of the above, Applicants submit that the application is now in condition for allowance and respectfully urge the Examiner to pass this case to issue.

***

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 12-0415. In particular, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 12-0415.

I hereby certify that this document is being transmitted to the Patent and Trademark Office via electronic filing.

April 18, 2011
(Date of Transmission)

Lonnie Louie
(Name of Person Transmitting)

/Lonnie Louie/
(Signature)

/Lee W. Tower/
Lee W. Tower
Attorney for Applicants
Reg. No. 30,229
LADAS & PARRY LLP
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300